

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

For additional information about this publication click this link.

<http://hdl.handle.net/2066/205621>

Please be advised that this information was generated on 2019-09-12 and may be subject to change.

Eigen schuld van de betrokkene bij een onrechtmatige verwerking van zijn persoonsgegevens

1. Inleiding

Indien een verwerkingsverantwoordelijke persoonsgegevens onrechtmatig verwerkt en deze verwerking leidt tot schade bij de betrokkene,¹ kan laatstgenoemde op basis van art. 82 Algemene Verordening Gegevensbescherming (AVG) een schadevergoeding vorderen.² In de literatuur over dit recht op schadevergoeding is de rol van de eigen verantwoordelijkheid van de betrokkene tot dusver onbesproken gebleven. In mijn optiek verdient die eigen verantwoordelijkheid meer aandacht. De betrokkene kan namelijk zelf bijdragen aan het veroorzaken of vergroten van de schade. Hij kan bijvoorbeeld (extra) schade hebben doordat hij niet onmiddellijk zijn wachtwoord wijzigt, terwijl de verwerkingsverantwoordelijke dit nadrukkelijk adviseert.³ Indien de schade “mede een gevolg is van een omstandigheid die aan de benadeelde kan worden toegerekend”, is er sprake van ‘eigen schuld’. Hierdoor kan op grond van art. 6:101 lid 1 BW de vergoedingsplicht van de aansprakelijke partij worden verminderd of zelfs in zijn geheel vervallen.

De vraag rijst onder welke omstandigheden een gedraging van de betrokkene kan leiden tot de toepassing van het leerstuk eigen schuld bij een onrechtmatige verwerking van zijn persoonsgegevens.⁴ In deze bijdrage beantwoord ik daarom de volgende onderzoeksvraag:

Wanneer kwalificeert een gedraging van de betrokkene als een “omstandigheid die aan de benadeelde kan worden toegerekend” in de zin van art. 6:101 lid 1 BW?

Ik onderzoek uitsluitend de vraag of de gedraging van de betrokkene kwalificeert als een ‘toerekenbare omstandigheid’ in de zin van art. 6:101 lid 1 BW. Eventuele problematiek met betrekking tot het csqn-verband tussen de gedraging van de betrokkene en de (extra) schade laat ik in dit artikel buiten beschouwing. Ik ga er steeds vanuit dat de toerekenbare omstandigheid heeft bijgedragen aan het ontstaan of het vergroten van de schade. Ook ga ik in deze bijdrage niet uitgebreid in op de causale schadeverdeling en de billijkheidscorrectie, die onderdeel zijn van de verdelingsfase van art. 6:101 lid 1 BW.⁵



Mr. T.F. Walree*

In paragraaf 2 beschrijf ik het leerstuk van eigen schuld. In paragraaf 3 toon ik aan waarom het gegevensbeschermingsrecht en een eigen schuld-verweer niet conflicteren. In paragraaf 4 behandel ik drie categorieën van gedrag van de

* Promovendus verbonden aan het Onderzoekcentrum Onderneming & Recht (OO&R) van de Radboud Universiteit. Tevens verbonden aan het Institute for Computing and Information Sciences (iCIS) van de Radboud Universiteit. (T.Walree@jur.ru.nl)

1. De definities van de begrippen ‘verwerkingsverantwoordelijke’, ‘betrokkene’, ‘persoonsgegevens’ en ‘verwerking’ zijn te vinden in art. 4 AVG.
2. Zie uitvoerig B. van Alsenoy, ‘Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation’, *JIPITEC* 2016, afl. 3, p. 282-283; T.F.E. Tjong Tjin Tai, ‘Aansprakelijkheid bij datalekken’, *WPNR* 2016/7110, p. 459-464; T.F. Walree, ‘De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens’, *WPNR* 2017/7172, p. 921-930; T.E. van der Linden & T.F. Walree, ‘De collectieve procedure als oplossing voor het privaatrechtelijke handhavingstekort bij een datalek?’, *AV&S* 2018/20, afl. 4, p. 105-113; N. Vrugt & W.F. Dammers, ‘Massaschadeclaims voor betrokkenen onder de AVG volgens Nederlands recht’, *Privacy & Informatie* 2018, afl. 4, p. 114-120; R. Dickmann, ‘Nach dem Datenabfluss: Schadenersatz nach Art. 82 der Datenschutz-Grundverordnung und die Rechte des Betroffenen an seinen personenbezogenen Daten’, *Recht und Schaden* 2018, afl. 7, p. 345-355.
3. *Kamerstukken II* 2012-2013, 33 662, nr. 3 (MvT), p. 9.
4. Concl. A-G Hartlief 23 november 2018, ECLI:NL:PHR:2018:1409 (overweging 3.14), bij HR 21 december 2018, ECLI:NL:HR:2018:2385.
5. Zie hierover A.L.M. Keirse, *Schadebeperringsplicht. Over eigen schuld aan de omvang van de schade* (diss.), Deventer: Kluwer 2003, p. 83-86; C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel II. De verbintenis in het algemeen, tweede gedeelte*, Deventer: Wolters Kluwer 2017, nr. 114.

betrokkene en bespreek ik wanneer dat gedrag (mogelijk) eigen schuld oplevert. In paragraaf 5 sluit ik af met een synthese en conclusie.

2. Leerstuk eigen schuld ex art. 6:101 lid 1 BW

Schade is niet altijd uitsluitend een gevolg van een doen of nalaten van de aangesprokene, maar kan ook mede voortvloeien uit een omstandigheid die voor risico van de benadeelde komt.⁶ In dat geval is er sprake van eigen schuld. Het leerstuk van eigen schuld is vastgelegd in art. 6:101 lid 1 BW. Dit artikel gaat uit van aansprakelijkheid van de schadeveroorzaker. Op basis van die aansprakelijkheid bestaat een vergoedingsplicht. Die vergoedingsplicht wordt echter verminderd of kan zelfs in zijn geheel komen te vervallen als de schade “mede een gevolg is van een omstandigheid die aan de benadeelde kan worden toegerekend”.

Eigen schuld vereist dus een ‘toerekenbare omstandigheid’. Het moet gaan om een gedraging van de benadeelde, dat kan zijn een handelen of nalaten, die bijdraagt aan het ontstaan en/of vergroten van de schade. Daarnaast omvat eigen schuld ook omstandigheden die naar verkeersopvattingen tot de risicosfeer van de benadeelde behoren.⁷ De term ‘eigen schuld’ heeft een ruimere strekking dan de term doet vermoeden en is dan ook niet letterlijk te vinden in art. 6:101 lid 1 BW.⁸

De bewijslast voor eigen schuld rust op de partij die zich erop beroept.⁹ De rechter beoordeelt of er sprake is van een toerekenbare omstandigheid aan de hand van de concrete omstandigheden en feiten van het geval.¹⁰ Niet elke omstandigheid die bijdraagt aan het ontstaan van de schade of de schade vergroot, levert eigen schuld op.¹¹ Dit is pas het geval als het gedrag van de benadeelde in de gegeven omstandigheden onzorgvuldig, normschendend of foutief was. Hiervan is sprake als de benadeelde anders kon en moest handelen met het oog op de bescherming van eigen persoon of goed.¹² Eigen schuld vereist geen onrechtmatigheid of het schenden van een verplichting naar een ander, en is in die zin dus geen spiegelbeeld van aansprakelijkheid.¹³

Een vorm van eigen schuld is de schadebeperkingsplicht. De ‘gewone’ eigen schuld heeft invloed op het ontstaan van de schade, terwijl een schending van de schadebeperkingsplicht invloed heeft op de omvang van de schade. De toerekenbare omstandigheid die van invloed is op de omvang van de schade kan ook liggen vóór het moment van het ontstaan van de schade-veroorzakende gebeurtenis.¹⁴ Voor het bestaan en de inhoud van een schade-

beperkingsplicht is beslissend of het beperken van de schade redelijkerwijs van de benadeelde kon worden verlangd.¹⁵ Kon de benadeelde redelijkerwijs de omvang van de schade beperken, maar heeft hij dit niet gedaan, dan is er sprake van een toerekenbare omstandigheid.

Een schending van de schadebeperkingsplicht leidt niet noodzakelijkerwijs tot een andere verdeling van de schade. De billijkheid in de verdelingsfase van art. 6:101 lid 1 BW kan namelijk vereisen dat de vergoedingsplicht van de aansprakelijke partij geheel in stand blijft.¹⁶ Dit speelt bijvoorbeeld indien zowel de aansprakelijke partij als de benadeelde de schade hadden kunnen beperken. In dit geval “hangt het van de omstandigheden van het geval

6. Asser/Sieburgh 6-II 2017/107; C.J.H. Jansen, ‘Eigen schuld van de benadeelde: historische wortels en toepassingsbereik van art. 6:101 BW naar aanleiding van D. 9, 2, 11, pr’, *RM Themis* 2002, afl. 4, p. 204-209.
7. Dit is bijvoorbeeld het geval waarin de schade mede is veroorzaakt door een persoon, dier of zaak waarvoor de benadeelde op grond van Boek 6 met een kwalitatieve aansprakelijkheid zou zijn belast, indien hierdoor schade aan een ander zou zijn toegebracht. Zie A.L.M. Keirse, ‘Rechterlijke werkzaamheid en het oordeel over eigen schuld’, *AV&S* 2006/30, afl. 6, p. 186-187.
8. Zie voor de verschillende interpretaties en discussie hierover de aangehaalde literatuur in A.L.M. Keirse & R.H.C. Jongeneel, *Eigen schuld en mede-aansprakelijkheid* (Monografieën Privaatrecht nr. 16), Deventer: Kluwer 2013, nr. 17. Zie ook Asser/Sieburgh 6-II 2017/107; R.J.B. Boonekamp, commentaar op art. 6:101 BW, in: A.T. Bolt (red.), *Groene Serie Schadevergoeding*, Deventer: Wolters Kluwer 2018, aant. 1.2.
9. HR 11 juni 2010, ECLI:NL:HR:2010:BM1733 (*Fortes e.a./Van der Bie*), r.o. 3.2.2.
10. Keirse 2003, p. 113. Zie bijvoorbeeld Hof Leeuwarden 29 maart 2006, ECLI:NL:GHLEE:2006:AV7749, r.o. 16.
11. De aangesprokene zou anders bijna altijd een beroep kunnen doen op een (gedeeltelijke) bevrijding van zijn aansprakelijkheid, zie Keirse & Jongeneel 2013, nr. 23.
12. Boonekamp 2018, aant. 2.2.1; Keirse 2003, p. 98-99; Keirse & Jongeneel 2013, nr. 17, 18, 23; Asser/Sieburgh 6-II 2017/107.
13. Keirse 2003, p. 97-98; Keirse & Jongeneel 2013, nr. 24, 26; Boonekamp 2018, aant. 1.6. Zie ook C.J. van Zeben, J.W. du Pon & M.M. Olthof (red.), *Parlementaire Geschiedenis van het nieuwe Burgerlijk Wetboek. Boek 6, Algemeen gedeelte van het verbintenissenrecht*, Deventer: Kluwer 1981, p. 352.
14. Keirse 2003, p. 43; Asser/Sieburgh 6-II 2017/125; Boonekamp 2018, aant. 5.2.1.
15. HR 5 oktober 1979, *NJ* 1980/43 (*Tauber/Verhey*); HR 5 december 2014, *NJ* 2016/159, ECLI:NL:HR:2014:3532, m.nt. S.D. Lindenbergh (*Michielsens/De Mierden*), r.o. 3.8.2.
16. Zie over de verdelingsfase Keirse 2003, p. 83-86; Asser/Sieburgh 6-II 2017/114.

af of en in hoeverre de vergoedingsplichtige aan de benadeelde kan tegenwerpen dat deze de schade niet heeft beperkt”. Daarbij moet in aanmerking worden genomen dat de benadeelde door een handelen of nalaten van de schadeveroorzaker in de situatie is beland die tot schadebeperking noodzaakt.¹⁷ Dit brengt met zich dat bij een dubbele mogelijkheid tot schadebeperking het in beginsel aan de schadeveroorzaker is om de schadebeperkende maatregel te initiëren.¹⁸ In dit geval is er dan mogelijk wel sprake van eigen schuld, maar leidt dit dus niet tot een andere verdeling van de schade.

3. Stelt het gegevensbeschermingsrecht beperkingen aan toepassing van eigen schuld?

3.1. Algemeen

Het gegevensbeschermingsrecht bevat uitsluitend verplichtingen voor de verwerkingsverantwoordelijke of ‘verwerker’¹⁹ van persoonsgegevens. Het legt geen enkele verplichting op aan de betrokkene. Door het ontbreken van die verplichtingen rijst daarom de vraag of het gegevensbeschermingsrecht wel ruimte biedt voor een eigen verantwoordelijkheid van de betrokkene, en dus of er ruimte is voor toepassing van het leerstuk van eigen schuld bij de handhaving van het gegevensbeschermingsrecht.

Ik betoog dat er wel degelijk een eigen verantwoordelijkheid voor de betrokkene bestaat, en dat het gegevensbeschermingsrecht ruimte biedt voor toepassing van eigen schuld. Ten eerste volgt het bestaan van een eigen verantwoordelijkheid uit de begrensde verantwoordelijkheid van de verwerkingsverantwoordelijke. Deze begrensde verantwoordelijkheid vloeit voort uit bepalingen in de AVG (paragraaf 3.2.). Ten tweede biedt het Unierecht ruimte voor toepassing van eigen schuld van de betrokkene, mits er geen sprake is van een schending van het effectiviteitsbeginsel (paragraaf 3.3.).

3.2. Eigen verantwoordelijkheid betrokkene volgt uit begrensde verantwoordelijkheid verwerkingsverantwoordelijke

Een eigen verantwoordelijkheid voor de betrokkene volgt indirect uit het feit dat de AVG een *risk-based approach* hanteert.²⁰ Die benadering gaat ervan uit dat het niveau van de maatregelen die de verwerkingsverantwoordelijke moet treffen, wordt gebaseerd op de risico’s die gepaard gaan met de gegevensverwerking.²¹ Tegelijkertijd stelt die benadering grenzen aan de verantwoordelijkheid van de verwerkingsverantwoordelijke. Die begrensde verantwoordelijkheid komt bijvoorbeeld tot uitdrukking in de

beveiligingsplicht ex art. 32 AVG. Dit artikel bepaalt dat de verwerkingsverantwoordelijke “passende technische en organisatorische maatregelen” moet nemen om “een op het risico afgestemd beveiligingsniveau te waarborgen”. Art. 32 AVG vereist niet dat de technische en organisatorische maatregelen moeten beschermen tegen *elke* onrechtmatige verwerking. Een inbreuk op de beveiliging van de verwerkingsverantwoordelijke duidt dus niet noodzakelijkerwijs op nalatigheid ten aanzien van de beveiligingsplicht.²² In die zin wordt de verantwoordelijkheid van de verwerkingsverantwoordelijke begrensd. Die begrenzing is niet onlogisch, aangezien een verwerkingsverantwoordelijke geen waterdichte beveiliging kan garanderen die beschermt tegen elk denkbaar scenario.²³

De begrensde verantwoordelijkheid van de verwerkingsverantwoordelijke volgt ook uit de disculpatieclausule in art. 82 lid 3 AVG. Deze clausule luidt: “Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.” De verwerkingsverantwoordelijke wordt bijvoorbeeld van aansprakelijkheid vrijgesteld als de schade het gevolg is van een fout van de betrokkene. Dit blijkt uit overweging 55 van de Dataprotectie-

17. HR 5 december 2014, NJ 2016/159, ECLI:NL:HR:2014:3532, m.nt. S.D. Lindenberg (Michiels/De Mierden), r.o. 3.8.2.

18. Keirse 2003, p. 118-134 (met name p. 124). Zie onder meer HR 9 mei 1986, NJ 1987/252 (Staat/Van Gelder); HR 28 september 2001, NJ 2001/650 (FDP/Leiden).

19. De verwerker is “een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt” (art. 4 sub 8 AVG).

20. Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN WP218, p. 1-4. Te raadplegen via: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf. Zie bijvoorbeeld R. Gellert, ‘Understanding the notion of risk in the General Data Protection Regulation’, *Computer Law & Security Review* 2018, afl. 2, p. 279-288.

21. Ook kan het hoge risico van de verwerking extra verplichtingen in het leven roepen voor de verwerkingsverantwoordelijke, zoals het uitvoeren van een ‘gegevensbeschermingseffectbeoordeling’ (art. 35 AVG).

22. Vgl. *Kamerstukken II* 1997-1998, 25 892, nr. 3 (MvT), p. 99.

23. Vgl. Hof Arnhem-Leeuwarden 4 september 2018, ECLI:NL:GHARL:2018:7967, r.o. 5.8.

richtlijn (de voorganger van de AVG).²⁴ Hierin staat, ten aanzien van de disculpatieclausule in art. 23 lid 2 van de Dataprotectierichtlijn, dat de (verwerkings)verantwoordelijke niet aansprakelijk is als hij bewijst dat er sprake is “van een fout van de betrokkene of van overmacht”. In de finale tekst van de AVG ontbreekt de overweging over een fout van de betrokkene. Dit is opmerkelijk, omdat die overweging wel stond in een eerdere versie.²⁵ Het is onduidelijk waarom deze passage is verdwenen. Er zijn geen aanwijzingen dat de disculpatieclausules van art. 23 lid 2 Dataprotectierichtlijn en art. 82 lid 3 AVG op verschillende manieren moeten worden uitgelegd.²⁶

Het gegevensbeschermingsrecht beoogt geen oneindige verantwoordelijkheid in het leven te roepen voor de verwerkingsverantwoordelijke. Deze begrenzing van de verantwoordelijkheid leidt tot een eigen verantwoordelijkheid voor de betrokkene. Het gegevensbeschermingsrecht gaat er immers vanuit dat de betrokkene in sommige situaties zelf het risico draagt van schade door misbruik van zijn persoonsgegevens. Ook in beleidsstukken veronderstellen de Nederlandse²⁷ en Europese²⁸ overheid een eigen verantwoordelijkheid van de betrokkene. In het licht van die eigen verantwoordelijkheid conflicteert de mogelijkheid van een eigen schuldverweer door de verwerkingsverantwoordelijke dus niet met de strekking en doelstellingen van het gegevensbeschermingsrecht.²⁹ Dat een eigen schuldverweer tot de mogelijkheden behoort, wordt zelfs expliciet bevestigd door staatssecretaris Teeven. Hij signaleert dat er mogelijk sprake kan zijn van eigen schuld als de betrokkene na een melding van een datalek geen gehoor geeft aan de door de (verwerkings)verantwoordelijke voorgestelde maatregelen.³⁰

3.3. Unierecht biedt ruimte voor eigen schuld van de betrokkene

Dat de AVG een Unierechtelijk instrument is, sluit toepassing van eigen schuld niet uit. De plicht voor een benadeelde om zijn schade zoveel mogelijk te beperken is namelijk een door het Hof van Justitie erkend ‘algemeen beginsel’.³¹ Bovendien verzet het Unierecht zich niet tegen een regel van nationaal recht die bepaalt dat een benadeelde geen of slechts een gedeeltelijke schadevergoeding kan vorderen omdat hij zelf heeft bijgedragen aan de schade. Het Unierecht verzet zich pas hiertegen indien het eigen schuldverweer in strijd is met het effectiviteitsbeginsel.³² Het effectiviteitsbeginsel brengt met zich dat het invoeren van een Unierechtelijke regel niet (vrijwel) onmogelijk mag worden gemaakt door het invoeren van een nationale regel.³³ Toepassing van het leerstuk van eigen schuld mag geen afbreuk doen aan het

24. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
25. Zie overweging 118 in de versie van 12 maart 2014 (EP-PE_TC1-COD(2012)0011). Te raadplegen via: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0/EN>.
26. Van Alsenoy 2016, p. 276, 283; P.T.J. Wolters, ‘De beveiliging van persoonsgegevens. Een geharmoniseerde verplichting of gedeelde verantwoordelijkheid?’, *SEW. Tijdschrift voor Europees en economisch recht* 2017, afl. 4, p. 153.
27. Het Ministerie van Veiligheid en Justitie stelt bijvoorbeeld in de Nationale Cybersecuritystrategie: “Van burgers wordt een zekere mate van cyberhygiëne (het toepassen van basis-veiligheidsvereisten) en een eigen verantwoordelijkheid verwacht.” Die verantwoordelijkheid bestaat uit het “voorzichtig zijn met persoonlijke gegevens, het uitvoeren van updates, het gebruik van sterke wachtwoorden”. Zie Ministerie van Veiligheid en Justitie, *De Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam*, 2013, p. 8, 20. Dit rapport is te raadplegen via: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cyber-security-strategie-2-2.pdf>
28. Ten aanzien van cybersecurity spreekt de Europese Commissie over “gedeelde verantwoordelijkheden” tussen overheden, de private sector, en individuen, en zegt de Commissie dat alle actoren zich moeten beschermen. Zie European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, p. 4.
29. Daarnaast sluit het feit dat ook een betrokkene soms (gedeeltelijk) zijn eigen schade moet dragen aan bij de oude gedachte dat het leerstuk van eigen schuld een compromis vormt tussen de twee in het buitencontractuele aansprakelijkheidsrecht tegen gestelde uitgangspunten, namelijk dat ‘ieder zijn eigen schade draagt’ en dat ‘onrechtmatig toegebrachte schade moet worden vergoed’. Zie L.E.H. Rutten, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. Derde deel – Verbintenissenrecht. Tweede stuk. De overeenkomst en de verbintenis uit de wet. Tweede gedeelte (slot)*, Zwolle: W.E.J. Tjeenk Willink 1954, p. 543.
30. *Kamerstukken II* 2012-2013, 33 662, nr. 3 (MvT), p. 9.
31. HvJ EG 5 maart 1996, C-46/93 en C-48/93 (*Brasserie du pêcheur/Bondsrepubliek Duitsland en Factortame/Verenigd Koninkrijk*), par. 85.
32. Vgl. HvJ EG 20 september 2001, C-453/99 (*Courage/Crehan*), par. 29; HvJ EG 16 december 1976, C-33/76 (*Rewe*), par. 5; HR 20 december 2013, ECLI:NL:HR:2013:2123, NJ 2014/347 m.nt. M.R. Mok & J. Hijma (*BP/Benschop c.s.*) 3.8.2.
33. M.M.C. van de Moosdijk, *Unjust enrichment in European Union Law* (diss. Nijmegen), Deventer: Wolters Kluwer 2018, p. 6-7 (voetnoot 21). Van de Moosdijk verwijst naar HvJ EG 16 december 1976, C-33/76, ECLI:EU:C:1976:188 (*Rewe*), par. 5; HvJ EG 16 december 1976, C-45/76, ECLI:EU:C:1976:191 (*Comet*), par. 12-16. Zie ook C.H. Sieburgh, ‘EU Law and Non-Contractual Liability of the Union, Member States and Individuals’, in: *The Influence of EU Law on National Private Law* (red. A.S. Hartkamp e.a.), Deventer: Kluwer 2014, p. 514-515.

beschermende doel van de geschonden regel van Unierecht.³⁴ Toepassing van eigen schuld mag er dus niet toe leiden dat de uitoefening van het recht op schadevergoeding bij een onrechtmatige verwerking van persoonsgegevens (in veel gevallen) onmogelijk wordt. Zolang hier geen sprake van is, sluit het Unierecht toepassing van eigen schuld niet uit.

Het feit dat de AVG uitsluitend verplichtingen adresseert aan de verwerkingsverantwoordelijke en de verwerker betekent ook niet dat er helemaal geen eigen verantwoordelijkheid kan bestaan voor de betrokkene. De AVG bepaalt namelijk *niet* dat de betrokkene geen verantwoordelijkheid heeft. De eventuele verantwoordelijkheid van de betrokkene valt buiten het bereik van de verordening. Een verantwoordelijkheid voor de betrokkene kan voortvloeien uit andere bepalingen, zoals het leerstuk van eigen schuld. Daarnaast bepaalt art. 82 AVG niets over de eigen schuld van de betrokkene. Het sluit de toepassing van dit leerstuk dus ook niet uit.

4. Welk gedrag van de betrokkene kan een toerekenbare omstandigheid opleveren?

4.1. Algemeen

In deze paragraaf onderzoek ik wanneer het schadeveroorzakende gedrag van de betrokkene kan worden aangemerkt als een toerekenbare omstandigheid in de zin van art. 6:101 lid 1 BW. Voor een toerekenbare omstandigheid is op zijn minst onzorgvuldig gedrag van de betrokkene vereist (paragraaf 2). Ten aanzien van het (onzorgvuldige) gedrag van de betrokkene maak ik een onderscheid in drie categorieën: de verwerkingsverantwoordelijke adviseert maatregelen maar de betrokkene volgt deze niet op (paragraaf 4.2.); een onzorgvuldig handelen van de betrokkene, zonder dat er sprake is van een advies van de verwerkingsverantwoordelijke (paragraaf 4.3.); de betrokkene nam geen anticiperende maatregelen (paragraaf 4.4.).³⁵ Bij het bespreken van het gedrag van de betrokkene ga ik telkens uit van aansprakelijkheid van de verwerkingsverantwoordelijke.³⁶

Ik begin met een algemene opmerking over de bruikbaarheid van de bestaande jurisprudentie. Door een schaarste aan (lagere en hogere) rechtspraak zijn er weinig aanknopingspunten voor de beantwoording van de vraag of er sprake is van een aan de betrokkene toerekenbare omstandigheid in de zin van art. 6:101 lid 1 BW. Er zijn mij slechts twee uitspraken bekend waarin een aansprakelijke verwerkingsverantwoordelijke die in strijd handelde met de Wet bescherming persoonsgegevens³⁷ een beroep deed op eigen schuld van de betrokkene.³⁸

Een vergelijking met andere situaties van eigen schuld is lastig. De algemene onrechtmatige daad-jurisprudentie geeft weinig bruikbare en praktische maatstaven voor de beoordeling of er sprake is van een toerekenbare omstandigheid.³⁹ De beoordeling van eigen schuld vindt immers plaats aan de hand van de concrete omstandigheden van het geval, waardoor de inkleuring daarvan casuïstisch van aard is. De toepassing van art. 6:101 lid 1 BW in de rechtspraak, bijvoorbeeld bij arbeidsongevallen⁴⁰ en bij de optiehandel of effectenlease,⁴¹ leent zich daarom slechts in beperkte mate voor het beoordelen van eigen schuld bij een onrechtmatige verwerking van persoonsgegevens.⁴² De vergelijking tussen het gegevensbeschermingsrecht en andere gevallen is bovenal lastig, omdat de veelal

34. Sieburgh 2014, p. 485-486.

35. Zie voor een vergelijkbare methode van categorisering van eigen schuld L.C. Dufour & H.J. Delhaas, 'Eigen schuld verweer van de aansprakelijkgestelde notaris; een kwestie van gevoel?', *WPNR* 2018/7191, p. 348-354.

36. Zonder aansprakelijkheid van de wederpartij van de benadeelde komt de rechter immers niet toe aan toepassing van art. 6:101 BW.

37. De Wet bescherming persoonsgegevens was de implementatie van de Dataprotectierichtlijn.

38. Hof 's-Gravenhage 16 februari 2007, ECLI:GHSGR:2007:BA1567 (*Kluwer/X*), r.o. 4.7 (eigen schuld-verweer werd toegekend); Rb. Utrecht 12 augustus 2009, ECLI:NL:RBUTR:2009:BJ5273 (*X/Agis*), r.o. 4.6 (eigen schuld-verweer werd afgewezen).

39. C.E.C. Jansen, 'Toerekening van 'eigen schuld' in het contractenrecht', in: *Tussen 'Alles' en 'Niets'. Van toedeling naar verdeling van nadeel*, (red. W.H. van Boom, C.E.C. Jansen & J.G.A. Linssen), Deventer: W.E.J. Tjeenk Willink 1997, p. 45; Keirse 2006, p. 185.

40. Zie onder meer HR 9 januari 1987, ECLI:NL:HR:1987:AG5504, NJ 1987/948 m.nt. P.A. Stein (*Beijzeldelooptkat*), r.o. 3.2; HR 20 september 1996, ECLI:NL:HR:1996:ZC2142, NJ 1997/198 m.nt. P.A. Stein (*Pollemans/Hoondert*), r.o. 3.4.

41. HR 23 mei 1997, ECLI:NL:HR:1997:AG7238, NJ 1998/192 m.nt. C.J. van Zeben (*Rabobank/Everaars*), r.o. 3.3; HR 5 juni 2009, ECLI:NL:HR:2009:BH2815, NJ 2012/182 m.nt. J.B.M. Vranken onder NJ 2012/184 (*De Treek/Dexia*), r.o. 4.16.2.

42. Ook laat een situatie waarin het gaat om een onrechtmatige verwerking van persoonsgegevens (en een fout van de betrokkene) zich bijvoorbeeld moeilijk vergelijken met gevallen waarin: een dronken eiser illegaal vuurwerk van een collega aansteekt en als gevolg daarvan letsel ondervindt (Rb. Noord-Holland 18 juli 2018, ECLI:NL:RBNHO:2018:6085 (*Cobra 6*), r.o. 4.10); eiser naliet onderzoek te doen naar de waarde en de bestemming van de grond die hij wilde kopen (Hof Arnhem-Leeuwarden 26 november 2013, ECLI:NL:GHARL:2013:8997 (*X/Keizer & Van Goor Notarissen*), r.o. 2.10); en een drone van eiser wordt neergeschoten door de buurman die zich bispied waande (Rb. Gelderland 10 mei 2017, ECLI:NL:RBGEL:2017:2663 (*Neergeschoten drone*), r.o. 2.6).

immateriële en abstracte gevolgen van bijvoorbeeld een datalek of een ongeïnformeerde gegevensverwerking op een ander niveau liggen dan bijvoorbeeld inbreuken op de fysieke integriteit of inbreuken die een duidelijkere impact hebben op het vermogen van de benadeelde.⁴³ Ten aanzien van fysiek waarneembare schade of schade die direct de portemonnee treft, is het bovendien meestal een stuk duidelijker wat de benadeelde had kunnen of moeten doen om schade te voorkomen of te beperken.

4.2. De verwerkingsverantwoordelijke adviseert maatregelen maar de betrokkene volgt deze niet op

Een verwerkingsverantwoordelijke kan een betrokkene adviseren om zelf een schadebeperkende maatregel te nemen, zoals het wijzigen van een wachtwoord nadat het wachtwoord van de betrokkene (mogelijk) is ingezien bij een datalek.⁴⁴ Een dergelijk advies kan worden ingegeven door: (i) de wettelijke meldplicht op grond van art. 34 AVG; (ii) de beveiligingsplicht op grond van art. 32 AVG; (iii) de meer algemene informatie- of waarschuwingsplicht bij gevaarzettingssituaties.

De meldplicht op grond van art. 34 lid 1 AVG ontstaat als er een (niet uit te sluiten) datalek is dat “waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden” van de betrokkene. In dit geval is de verwerkingsverantwoordelijke verplicht het datalek ‘onverwijld’ te melden aan de betrokkene. Deze melding vereist dat de verwerkingsverantwoordelijke maatregelen voorstelt of neemt om de onrechtmatige verwerking aan te pakken of, indien dat mogelijk is, maatregelen voorstelt of neemt om de eventuele nadelige gevolgen van de onrechtmatige verwerking te beperken (art. 34 lid 2 en art. 33 lid 3 sub d AVG). Een maatregel die de verwerkingsverantwoordelijke bijvoorbeeld kan treffen, is het geven van advies aan de betrokkene over schadebeperkende maatregelen die de betrokkene zelf kan nemen.

Een informatieplicht voor de verwerkingsverantwoordelijke kan ook voortvloeien uit art. 32 AVG. Dit artikel verplicht de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beschermen tegen bijvoorbeeld verlies of onbevoegde kennisname. Een organisatorische maatregel kan bijvoorbeeld inhouden dat de verwerkingsverantwoordelijke, gelet op de risico’s van de gegevensverwerking, de betrokkene proactief moet informeren over de specifieke risico’s die gepaard gaan met de verwerking van zijn persoonsgegevens en moet adviseren over de wijzen waarop deze risico’s kunnen

worden verkleind. Een dergelijke verplichting kan ook worden gebaseerd op een algemene waarschuwingsplicht bij gevaarzettingssituaties op grond van het ongeschreven recht.⁴⁵

Het waarschuwen van de betrokkene of het adviseren over te nemen schadevoorkomende of schadebeperkende maatregelen door de aansprakelijke verwerkingsverantwoordelijke leidt niet direct tot eigen schuld, indien de betrokkene de geadviseerde maatregel niet opvolgt en als gevolg daarvan schade ontstaat. Er is pas sprake van eigen schuld als de verwerkingsverantwoordelijke de betrokkene dusdanig informeerde of waarschuwde, dat de betrokkene moest begrijpen dat hij anders kon en had moeten handelen. De gemiddelde betrokkene⁴⁶

43. O. Lynskey, ‘The Foundations of EU Data Protection Law’, Oxford: Oxford University Press 2015, p. 196-228; E. Descheemaeker, ‘The Harms of Privacy’, *Journal of Media Law* 2016, afl. 8, p. 278-306; D.J. Solove & D.K. Citron, ‘Risk and Anxiety: A Theory of Data Breach Harms’, *Texas Law Review* 2018, p. 755.

44. Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN WP250rev.01, p. 20. Te raadplegen via: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Zie ook *Kamerstukken II* 2012-2013, 33 662, nr. 3 (MvT), p. 22; F. van der Jagt, ‘Tets te melden? De diverse datalek-meldplichten in kaart gebracht’, *NJB* 2012/1415, afl. 25; Tjong Tjin Tai 2016, p. 461.

45. Vgl. HR 5 november 1965, *NJ* 1966/136 (*Kelderluik*). Zie uitvoerig over informatieplichten bij datalekken en beveiligingsinbreuken: J.A.N. Baas & M.H.J. van Rest, ‘Informatie- en meldplichten bij datalekken en beveiligingsinbreuken’, *Privacy & Informatie* 2012, afl. 6, p. 260-268. Zie over de informatieplicht in het algemeen: K.J.O. Jansen, *Informatieplichten: over kennis en verantwoordelijkheid in contractenrecht en buitencontractueel aansprakelijkheidsrecht* (diss. Leiden), Deventer: Kluwer 2012.

46. Ik verwacht dat de hoedanigheid (zoals werknemer of bestuurder) en/of capaciteiten (zoals kennis van IT) van de betrokkene er niet sneller toe leiden dat er sprake is van een toerekenbare omstandigheid (vgl. Keirse 2006 (p. 186) en Keirse & Jongeneel 2013 (nr. 27) over de rol van subjectieve factoren bij de beoordeling of er sprake is van een toerekenbare omstandigheid). Een verwerkingsverantwoordelijke heeft immers als organisatie vrijwel altijd meer informatie tot zijn beschikking dan de individuele betrokkene. Aan de andere kant kan de kwetsbare positie van de betrokkene (zoals een kind) met zich brengen dat er juist geen sprake is van een toerekenbare omstandigheid. Vgl. in andere zin bij beroepsaansprakelijkheid voor (letselschade) advocaten I. Giesen, ‘Aansprakelijkheid van de (letselschade) advocaat voor informatieverzuimen: het bewijs van de zorgplichtschending en de (ontbrekende) eigen schuld van de cliënt’, *Tijdschrift voor Vergoeding Personenschade* 2016, afl. 2, p. 42 (voetnoot 46).

is echter ondeskundig⁴⁷ en ongeïnformeerd,⁴⁸ terwijl het doorgronden van en het adequaat reageren op een waarschuwing of melding een bepaald niveau van kennis, alertheid en zelfcontrole vereist.⁴⁹ Daarnaast kan de betrokkene de gevolgen van de gegevensverwerking over het algemeen moeilijk overzien.⁵⁰ Hij heeft aanzienlijk minder kennis over de (voorzienbare risico's van de) gegevensverwerking dan de verwerkingsverantwoordelijke.⁵¹ Doordat de verwerkingsverantwoordelijke de gegevensverwerking initieert en faciliteert, is de betrokkene afhankelijk van de informatie die de verwerkingsverantwoordelijke hem verschaft.

Voordat het gedrag van de betrokkene (het niet opvolgen van een geadviseerde maatregel) kwalificeert als onzorgvuldig en dus aan hem is toe te rekenen in de zin van art. 6:101 lid 1 BW, is het niet alleen vereist dat een verwerkingsverantwoordelijke de betrokkene tijdig heeft geïnformeerd, gewaarschuwd of heeft geadviseerd. Daarnaast is nodig dat het voor de betrokkene op basis van de verstrekte informatie duidelijk is dat hij moet handelen en hoe hij moet handelen. De kwaliteit van de waarschuwing of het advies is daarom richtinggevend voor het antwoord op de vraag of de betrokkene onzorgvuldig handelde. Is het advies over de risico's en de te nemen maatregelen "duidelijk en in niet te mis verstane bewoordingen", dan is het gedrag van een betrokkene eerder onzorgvuldig dan wanneer een advies van de verwerkingsverantwoordelijke ontbreekt of wanneer een advies onvolledig, niet-concreet of onduidelijk was.⁵²

De vraag rijst wanneer een waarschuwing of advies zo duidelijk is dat het niet opvolgen daarvan onzorgvuldig is. De AVG biedt voor het antwoord op deze vraag weinig aanknopingspunten. Zij vergt slechts dat de melding aan de betrokkene "in duidelijke en eenvoudige taal" is,⁵³ en dat de melding ten minste bevat "de waarschijnlijke gevolgen" van het beveiligingsincident⁵⁴ en "de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan."⁵⁵

Ik doe daarom een suggestie voor gezichtspunten. Voor de beoordeling of de betrokkene onzorgvuldig handelde, omdat hij het advies van de verwerkingsverantwoordelijke niet opvolgde (en daardoor schade ontstond of werd vergroot), stel ik voor dat de rechter onderzoekt of de betrokkene, aan de hand van de ontvangen melding en het advies van de verwerkingsverantwoordelijke, moest begrijpen: (i) dat er een

concreet risico voor hem bestond; (ii) dat zijn specifieke handelen noodzakelijk was om dat risico te beperken en dat het risico zou blijven bestaan als hij het advies niet opvolgde; (iii) wat de geadviseerde maatregel inhield en hoe hij deze kon nemen. Ook moet de rechter onderzoeken (iv) of de geadviseerde maatregel praktisch uitvoerbaar is voor de betrokkene. Daarnaast kan een rechter in oogschouw nemen: (v) of de betrokkene een redelijke termijn is gegeven om de maatregel op te volgen; (vi) op welk tijdstip de waarschuwing is gegeven (vóór of na het incident); (vii) of er een herhaalde waarschuwing is gegeven; (viii) of het gaat om een algemene of een aan de persoon gerichte waarschuwing.⁵⁶ Indien het bovenstaande tot de conclusie leidt dat de betrokkene onzorgvuldig handelde, en zijn gedrag mede bijdroeg aan de schade, is de eigen schuld gevestigd. Evenwel leidt de vestiging van eigen schuld niet automatisch tot een andere verdeling van de schade. De rechter kan immers tijdens de verdelingsfase van art. 6:101 lid 1 BW tot de conclusie komen dat er toch geen andere verdeling van de schade moet plaatsvinden en dat de vergoedingsplicht (ondanks de aanwezigheid van eigen schuld) in zijn geheel in

47. Vgl. T. Jacquemain, *Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht. Unter besonderer Berücksichtigung der Schadensbemessung*, Baden-Baden: Nomos Verlagsgesellschaft 2017, p. 247.

48. G. González Fuster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *IDP Revista de Internet, Derecho y Política* 2014, afl. 19, p. 92-104.

49. Vgl. S. Romanosky & A. Acquisti, 'Privacy Costs and Personal Data Protection: Economic and Legal Perspectives', *Berkeley Technology Law Journal* 2009, afl. 3, p. 1095-1096. Ook kan de betrokkene ongewoon vaak raken voor meldingen, omdat hij veelvuldig over datalekken is geïnformeerd, maar nadelige gevolgen altijd uitbleven.

50. P.T.J. Wolters, 'De rechten van de betrokkene onder de AVG', *Tijdschrift voor Consumentenrecht en handelspraktijken*, 2018, afl. 3, p. 131 (voetnoot 13).

51. Wolters 2018, p. 131; Van Alsenoy 2016, p. 275; P. de Hert e.a., 'The proposed Regulation and the construction of a principles-driven system for individual data protection', *The European Journal of Social Science Research* 2013, afl. 1-2, p. 141.

52. Vgl. HR 5 juni 2009, ECLI:NL:HR:2009:BH2815, *NJ 2012/182 (De Treek/Dexia)*.

53. Art. 34 lid 2 AVG.

54. Art. 34 lid 2 AVG jo. art. 33 lid 2 sub c AVG.

55. Art. 34 lid 2 AVG jo. art. 33 lid 2 sub d AVG.

56. Vgl. R.E. van Esch, 'Phishing en de waarschuwingsplicht van een bank: een drieluik', *Tijdschrift voor Financieel Recht* 2015, afl. 4, p. 129-130.

stand blijft, omdat de billijkheid dit wegens de uiteenlopende ernst van de gemaakte fouten of andere omstandigheden van het geval eist. Dit speelt bijvoorbeeld als zowel de betrokkene als de verwerkingsverantwoordelijke het in de hand hadden om de schade te voorkomen of te beperken. Als dit het geval is, moet de rechter aan de hand van de omstandigheden van het geval beoordelen in hoeverre het aan de betrokkene is toe te rekenen dat hij zijn schade niet heeft voorkomen of heeft beperkt. Bij die beoordeling moet in aanmerking worden genomen dat de benadeelde door een fout van de verwerkingsverantwoordelijke in de situatie is beland die tot schadebeperking noodzaakt.⁵⁷ Dit leidt tot het uitgangspunt dat, als beide partijen de mogelijkheid hebben om de schade beperken of te voorkomen, het in principe aan de verwerkingsverantwoordelijke is om het initiatief tot schadebeperking te nemen. Doet de verwerkingsverantwoordelijke dit niet, dan ligt het niet voor de hand dat er een andere verdeling van de schade plaatsvindt of dat de vergoedingsplicht in zijn geheel vervalt, ondanks dat ook de betrokkene zijn eigen schade had kunnen voorkomen of beperken.

Stel dat een verwerkingsverantwoordelijke de betrokkene informeert over een datalek waarbij een kwaadwillende mogelijk wachtwoorden heeft ingezien. De verwerkingsverantwoordelijke adviseert de betrokkene met klem om zijn wachtwoord te wijzigen. De betrokkene wijzigt zijn wachtwoord desondanks niet. Vervolgens wordt met het gestolen wachtwoord op het account van de betrokkene ingelogd door criminelen. Hierdoor ontstaat schade. Ervan uitgaande dat de betrokkene op grond van de melding moest begrijpen wat voor hem de concrete risico's waren en dat hij moest begrijpen dat zijn handelen noodzakelijk was om schade te voorkomen of te beperken, kan dit stilzitten van de betrokkene kwalificeren als een toerekenbare omstandigheid. Een dergelijk geval kan echter niet leiden tot een andere verdeling van de schade, omdat het wijzigen van een wachtwoord niet iets is dat uitsluitend de betrokkene kan doen. Het is namelijk technisch mogelijk voor een verwerkingsverantwoordelijke om een account te blokkeren zolang de betrokkene geen nieuw wachtwoord instelt. De verwerkingsverantwoordelijke kan de betrokkene een e-mail sturen met een link naar de webpagina waar de betrokkene een nieuw wachtwoord kan instellen en waarmee hij zijn account deblokkeert.⁵⁸

Een andere verdeling van de schade ligt meer voor de hand als het gaat om een geadviseerde maatregel of handeling die, althans in verhou-

ding tot de verwerkingsverantwoordelijke, uitsluitend de betrokkene kan nemen.

Een eerste voorbeeld is het geval waarin de verwerkingsverantwoordelijke de betrokkene na een datalek adviseert om ook zijn wachtwoorden te wijzigen bij andere organisaties. De kans is immers aanwezig dat de betrokkene één wachtwoord gebruikt voor verschillende accounts, en dat zijn gestolen wachtwoord ook wordt misbruikt bij accounts van andere organisaties.⁵⁹ Overigens kan de aansprakelijke verwerkingsverantwoordelijke betogen dat het gebruiken van eenzelfde wachtwoord voor verschillende accounts ook onvoorzichtig is zonder waarschuwing van hem. Dit betekent echter niet dat er sprake is van een toerekenbare omstandigheid in de zin van art. 6:101 BW. Zonder waarschuwing door de verwerkingsverantwoordelijke is het risico voor de betrokkene namelijk nog niet concreet.

Een tweede voorbeeld is de volgende casus. Na een datalek adviseert verzekeraar Top Verzekerd de betrokkene uitdrukkelijk om: (i) waakzaam te zijn voor verdachte e-mails; (ii) absoluut geen bijlagen met onbekende inhoud te openen aangezien deze kwaadaardige software kunnen bevatten; (iii) het e-mailadres van de afzender te controleren. Op basis van de gestolen gegevens verzendt een cybercrimineel vanaf info@topverzekerd.nl een persoonlijk gerichte e-mail aan de betrokkene, met bijgevoegd een geïnfecteerd pdf-bestand. De betrokkene opent het bestand, waardoor er vervolgens automatisch ransomware⁶⁰ op zijn computer wordt

57. HR 5 december 2014, *NJ* 2016/159, ECLI:NL:HR:2014:3532, m.nt. S.D. Lindenbergh (*Michiels/De Mierden*), r.o. 3.8.2.

58. Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN WP250rev.01, p. 32.

59. Het is een bekend probleem dat gebruikers van onlinediensten één wachtwoord gebruiken voor meerdere accounts, zie C. Wang e.a., 'The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services', *CODASPY '18 Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, p. 196-203. Te raadplegen via: <https://people.cs.vt.edu/gangwang/pass.pdf>. Zie ook: <https://veiliginternetten.nl/nieuws/slechts-de-helft-van-de-nederlanders-weet-hoe-zich/>.

60. Zie uitvoerig over ransomware: B.H.M. Custers, J.J. Oerlemans & R.L.D. Pool, 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 2016, afl. 2, p. 87-95.

geïnstalleerd. Dit zorgt ervoor dat de betrokkene geen toegang meer heeft tot zijn computer en alle daarop opgeslagen bestanden. De computer wordt weer ontgrendeld als de betrokkene 0,5 Bitcoin overmaakt naar de crimineel. De betrokkene betaalt, en wil een schadevergoeding van de verwerkingsverantwoordelijke voor de geleden schade.

In de laatste twee voorbeelden is het verdedigbaar dat de betrokkene onzorgvuldig handelde. De verwerkingsverantwoordelijke waarschuwde immers voldoende voor de concrete risico's en adviseerde de betrokkene om specifiek te handelen om op bepaald handelen achterwege te laten, om zodoende het risico op misbruik te beperken. De betrokkene moest begrijpen dat hij anders had moeten handelen. Daarnaast gaat het in beide voorbeelden om een situatie waarin het uitsluitend de betrokkene was die 'iets' kon doen om de schade te beperken of te voorkomen.

4.3. Een onzorgvuldig handelen van de betrokkene (zonder dat er sprake is van een advies van de verwerkingsverantwoordelijke)

Een waarschuwing of advies van de verwerkingsverantwoordelijke aan de betrokkene is niet altijd noodzakelijk voor het aannemen van onzorgvuldig gedrag. Ook zonder een waarschuwing of advies kan de betrokkene onzorgvuldig handelen. Dit kan het geval zijn als het risico ook voor de niet-oplettende betrokkene aanstonds duidelijk had moeten zijn en hij moest begrijpen dat hij onder de gegeven omstandigheden anders had moeten handelen.⁶¹ Er zijn verschillende situaties denkbaar waarin de betrokkene ook zonder een advies of waarschuwing onzorgvuldig kan handelen, en daarmee bijdraagt aan het ontstaan of het vergroten van de schade. Dit betreft onder meer de situatie waarin de betrokkene: (i) gevoelige persoonsgegevens deelt; (ii) opzettelijk onjuiste persoonsgegevens verstrekt; (iii) bewust bijdraagt aan het openbaar worden van zijn persoonsgegevens of zelf de publiciteit opzoekt; (iv) ingaat op een kennelijk frauduleus verzoek.

i. De betrokkene deelt gevoelige persoonsgegevens
Allereerst kan de gevoelige aard van persoonsgegevens met zich brengen dat de betrokkene had moeten begrijpen dat hij anders had moeten handelen. Een voorbeeld is het geval waarin de betrokkene een foto van zijn net behaalde rijbewijs deelt op sociale media. Een kwaadwillende maakt een kopie van deze foto en verkoopt deze via het *dark web*. Vervolgens misbruikt een onbekende persoon de kopie om in dienst te kunnen treden bij de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke verifieert echter niet of deze persoon daadwerkelijk de

persoon is op de kopie van het rijbewijs, en neemt de gegevens van de betrokkene klakkeloos over voor de loonadministratie. Dientengevolge ontvangt de betrokkene ten onrechte vorderingen tot terugbetaling van toeslagen. De betrokkene spreekt de verwerkingsverantwoordelijke aan voor de schade omdat hij de identiteitsgegevens niet adequaat controleerde, en daarom in strijd handelde met de zorgvuldigheid die van hem als werkgever in het maatschappelijk verkeer mag worden verwacht.⁶² De verwerkingsverantwoordelijke verweert zich met een beroep op eigen schuld, omdat de betrokkene door het online zetten van zijn rijbewijs bijdroeg aan het ontstaan van de schade. In een dergelijk geval is eigen schuld niet ondenkbaar. De betrokkene had moeten begrijpen dat het delen van gegevens met een dergelijk gevoelige aard een hoog risico op schade met zich brengt. De betrokkene had met die wetenschap anders moeten handelen, en had die gegevens niet moeten delen via sociale media.

Niet valt uit te sluiten dat een kwaadwillende niet-gevoelige gegevens combineert die afkomstig zijn van zowel de verwerkingsverantwoordelijke als van de betrokkene.⁶³ Door die combinatie kunnen nieuwe (gevoelige) persoonsgegevens ontstaan of kunnen anonieme gegevens herleidbaar worden, waardoor schade kan ontstaan bij de betrokkene.⁶⁴ In een dergelijk scenario is het onredelijk om de betrokkene onzorgvuldig gedrag te verwijten. De betrokkene kan immers niet voorzien dat het (online) delen van niet-gevoelige informatie, die op zichzelf geen schade veroorzaakt, kan worden gecombineerd met

61. Vgl. HR 26 september 2003, NJ 2003/660 (*Waterschap Zeeuwse eilanden/Royal Nederland Verzekeringen*), r.o. 3.7. Vgl. K.J.O. Jansen, 'De eigen verantwoordelijkheid van de financiële consument', WPNR 2010/6853, p. 623.

62. Dit voorbeeld is deels ontleend aan Rb. Noord-Holland 28 december 2016, ECLI:NL:RBNHO:2016:10635 (*X/Van Hees*), r.o. 5.2.

63. Daarnaast is het mogelijk dat de verwerkingsverantwoordelijke en de betrokkene dezelfde gevoelige gegevens lekten. In dit geval kan het leerstuk van 'proportionele aansprakelijkheid' worden toegepast. Zie hierover Walree 2017, p. 924.

64. In de literatuur wordt dit fenomeen aangeduid als het 'problem of aggregation' of het 'aggregation effect'. Zie D.J. Solove, 'Privacy self-management and the consent dilemma', *Harvard Law Review* 2013, p. 1889-1890; N.N. Purtova, *Property rights in personal data: A European perspective* (diss. Tilburg), Oisterwijk: BOXPress BV 2011, p. 46, 118; Solove & Citron 2018, p. 775-776.

andere informatie die bijvoorbeeld afkomstig is van een 'lekkende' verwerkingsverantwoordelijke. Het aantal combinaties van gegevens en de mogelijke uitkomsten daarvan zijn bovendien gigantisch, waarop de betrokkene onmogelijk kan anticiperen. Het gedrag van de betrokkene is pas onzorgvuldig als het voor hem aanstonds duidelijk was dat er aanzienlijke kans bestond dat de specifieke gegevens, die hij in de openbaarheid deelde, konden worden gecombineerd met andere persoonsgegevens van hem, en dat er zodoende schade zou kunnen ontstaan. Hij had dus moeten begrijpen dat hij anders had moeten handelen. Een betrokkene kan nadelige gevolgen alleen voorzien bij het eigenhandig (online) verspreiden van gevoelige gegevens, zoals bijzondere persoonsgegevens (art. 9 AVG) of financiële persoonsgegevens, waarvan duidelijk is dat het verspreiden daarvan op zichzelfstaand al een hoog risico met zich brengt.⁶⁵

ii. De betrokkene verstrekt opzettelijk onjuiste persoonsgegevens

Ook kan er sprake zijn van onzorgvuldig gedrag als de betrokkene opzettelijk onjuiste gegevens aan de verwerkingsverantwoordelijke verstrekt.⁶⁶ Een voorbeeld waarin dit mogelijk kan leiden tot eigen schuld is de volgende situatie. De verwerkingsverantwoordelijke maakt, buiten de doeleinden van de oorspronkelijke verwerking, een profiel op van de betrokkene. Dit doet de verwerkingsverantwoordelijke op basis van onjuiste gegevens die de betrokkene opzettelijk aan hem verstrekte ten behoeve van de oorspronkelijke, rechtmatige gegevensverwerking. Door het 'onverenigbare' gebruik van de persoonsgegevens schendt de verwerkingsverantwoordelijke het principe van doelbinding (art. 5 lid 1 sub b AVG). Stel dat een betrokkene opzettelijk onjuiste persoonsgegevens verstrekte over zijn vermogenstoestand, bijvoorbeeld over het feit dat hij zogenaamd in de schuldsanering zit. Op basis van dat profiel doet de verwerkingsverantwoordelijke de betrokkene een schriftelijk aanbod tot rechtsbijstand. Dit kan leiden tot immateriële schade, omdat de betrokkene schrikt of geëmotioneerd is door de brief met het aanbod tot rechtsbijstand.⁶⁷ Mogelijk kan de verwerkingsverantwoordelijke dan een beroep doen op eigen schuld van de betrokkene, omdat hij de gegevens van de betrokkene verwerkte en hem vervolgens benaderde op basis van de door de betrokkene opzettelijk onjuist verstrekte persoonsgegevens.

iii. De betrokkene draagt bewust bij aan het openbaar worden van zijn persoonsgegevens of zoekt zelf de publiciteit op

In de rechtspraak omtrent onrechtmatige perspublicaties komt het voor dat de rechter

oordeelt dat er sprake is van eigen schuld, omdat de onrechtmatige en schadeveroorzakende publicatie (mede) het gevolg is van het feit dat de benadeelde zelf de publiciteit opzocht of het gevolg is van informatie die de benadeelde zelf bewust in de openbaarheid bracht.⁶⁸ Zo oordeelde de rechter bijvoorbeeld dat een zedendelinquent, in het geval dat de gemeente onrechtmatig handelde door het bekendmaken van zijn woonlocatie, eigen schuld had, omdat hij "de eerste stap heeft gezet in het mogelijk openbaar worden van zijn woonlocatie door contact te zoeken met een journalist en op zijn weblog informatie over zijn woonsituatie te publiceren".⁶⁹ Dat kan dus betekenen dat een rechter sneller tot het oordeel komt dat een betrokkene eigen schuld heeft bij de onrechtmatige verspreiding van zijn persoonsgegevens, indien de betrokkene zelf bijdroeg aan het openbaar worden van zijn persoonsgegevens of zelf de publiciteit opzocht.

iv. De betrokkene gaat in op een kennelijk frauduleus verzoek

Het ingaan op een frauduleus verzoek door de betrokkene kan ook kwalificeren als onzorgvuldig gedrag. Een gevolg van een datalek kan zijn dat een crimineel met behulp van de buitgemaakte persoonsgegevens de betrokkene benadert met een frauduleus verzoek, bijvoorbeeld door middel van *phishing*.⁷⁰ Het kan voorkomen dat een betrokkene op het moment

65. Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN WP250rev.01, p. 24.

66. Hof 's-Gravenhage 16 februari 2007, ECLI:GHSGR:2007:BA1567 (*Kluwer/X*), r.o. 4.7. Vgl. Rb. Rotterdam 19 september 2018, ECLI:NL:RBROT:2018:8292 (*X/Quion 50 B.V.*), r.o. 7.6; HR 14 december 2018, ECLI:NL:HR:2018:2298 (*Hyperinvest/X*). Vgl. ook M.R.L. Ruesen, 'Ongeschikte medische apps: wie is aansprakelijk?', *Computerrecht* 2017/49, afl. 2, p. 67-72; S.F. Thiems, 'Het elektronisch patiëntendossier: aansprakelijkheid als het misgaat', *Computerrecht* 2011/155, afl. 6, p. 311-319; S.A.L. van de Sande, *Overheidsaansprakelijkheid voor het verstrekken van onjuiste informatie* (diss. Nijmegen), Deventer: Wolters Kluwer 2019, p. 385-388.

67. Rb. Noord-Nederland 3 mei 2017, ECLI:NL:RBNNE:2017:1700 (*X/Advocatenkantoor*).

68. Rb. Amsterdam 22 november 2006, ECLI:NL:RBAMS:2006:AZ2849 (*X/Talpa*), r.o. 5.4. Vgl. Rb. Amsterdam 17 april 2008, ECLI:NL:RBAMS:2008:BC9778 (*Fitna*), r.o. 4.9.

69. Rb. Midden-Nederland 8 april 2015, ECLI:NL:RBMNE:2015:2329 (*X/Gemeente Amersfoort*), r.o. 4.9.

70. Voor een definitie van phishing, zie bijvoorbeeld Van Esch 2015, p. 129.

dat hij een dergelijk frauduleus verzoek ontvangt (nog) niet door de verwerkingsverantwoordelijke op de hoogte is gebracht van het datalek.⁷¹ Dat een betrokkene niet op de hoogte is gebracht over een datalek met zijn persoonsgegevens, neemt niet weg dat hij alsnog onzorgvuldig kan handelen door in te gaan op een frauduleus verzoek.

Een betrokkene handelt ten eerste onzorgvuldig als het voor hem aanstonds duidelijk was dat het om een frauduleus verzoek ging. Een verzoek kan bijvoorbeeld door de aanhef, opmaak, stijl, het taalgebruik of afzenderadres⁷² evident frauduleus zijn. Hierdoor had zelfs de niet-oplettende betrokkene moeten begrijpen dat hij te maken had met een frauduleus verzoek. Stel dat een bank zijn beveiliging niet op orde heeft. Hierdoor hebben criminelen toegang tot de NAW-gegevens, het klantnummer en e-mailadres van de betrokkene. De criminelen gebruiken die gegevens om de betrokkene te benaderen via een phishing-mail, waarbij de criminelen zich voordoen als de bank. In de e-mail wordt de betrokkene ten behoeve van 'de actualisering van de klantgegevens' door de 'bank' gevraagd om op een link te klikken. Op de pagina die opent, wordt de betrokkene gevraagd zijn inloggegevens voor internetbankieren in te vullen. De e-mail is niet persoonlijk geadresseerd aan de betrokkene, maar aan 'beste relatie'. De e-mail bevat diverse grammatica-, spel- en stijlfouten. Ook het afzenderadres komt niet overeen met de naam van de bank. De betrokkene vult desondanks zijn gegevens in, waaronder zijn inloggegevens. Met behulp van deze gegevens plunderen criminelen de rekening van de betrokkene.

Ten aanzien van dit specifieke geval is het verdedigbaar dat de betrokkene een dergelijk risico ook zonder waarschuwing moest herkennen. Het risico is moeilijker te herkennen indien de betrokkene in de e-mail ook wordt aangesproken met zijn naam en klantnummer. Het gedrag van de betrokkene kan dan alsnog onzorgvuldig zijn, omdat de risico's die zijn verbonden aan het afgeven van inloggegevens algemeen bekend is.⁷³ Het risico van het afgeven van inloggegevens kan bijvoorbeeld voor de betrokkene duidelijk zijn geweest door diverse mediacampagnes waarvoor dit specifieke risico is gewaarschuwd.⁷⁴

4.4. De betrokkene nam geen anticiperende maatregelen

Een derde categorie van mogelijk onzorgvuldig gedrag betreft situaties waarin de betrokkene anticiperende maatregelen kon en had moeten treffen om zich te beschermen tegen schade, maar dit niet deed. De schadebeperkingsplicht

kan namelijk met zich brengen dat een benadeelde vooraf anticiperende maatregelen had moeten treffen om schade te voorkomen of te beperken, zoals het dragen van een helm of veiligheidsgordel, zonder dat de aangesprokene waarschuwd voor potentieel gevaar.⁷⁵

Over het algemeen hoeft een betrokkene niet te anticiperen op een onrechtmatige verwerking van zijn persoonsgegevens. Een vrouw die onderdook met haar kinderen hoefde bijvoorbeeld niet te voorzien dat haar zorgverzekeraar geheime adresgegevens van haar kinderen zou prijsgeven aan haar ex-echtgenoot, en hoefde niet zelf om geheimhouding van de persoonsgegevens te vragen.⁷⁶ De betrokkene mag zonder enige informatie van de verwerkingsverantwoordelijke aannemen dat zijn persoonsgegevens zorgvuldig worden verwerkt.⁷⁷

Het uitgangspunt dat de betrokkene over het algemeen niet hoeft te anticiperen op een fout van de verwerkingsverantwoordelijke, gaat echter niet zover dat hij zich op geen enkele wijze hoeft te beschermen tegen nadelige gevolgen. Van de betrokkene kan worden verwacht dat hij beschikt over basale beveiligingsmaatregelen. Hij kan zich bijvoorbeeld

71. De betrokkene kan bijvoorbeeld worden benaderd door criminelen op het moment dat de verwerkingsverantwoordelijke nog niet op de hoogte is van het datalek, of voordat de verwerkingsverantwoordelijke de kans had om het datalek aan de betrokkene te melden. Daarnaast kan het voorkomen dat de betrokkene niet hoeft te worden gewaarschuwd. Dit kan bijvoorbeeld het geval zijn omdat de verwerkingsverantwoordelijke tijdens de risicoanalyse van het datalek gerechtvaardigd inschatte dat het onwaarschijnlijk was dat de risico's zich zouden verwezenlijken, en daarom niet aan de betrokkene hoefde te melden op grond van art. 34 AVG.

72. Vgl. Rb. Amsterdam 9 mei 2018, ECLI:NL:RBAMS:2018:2984 (*X/ABN Amro*), r.o. 4.8.

73. Van Esch 2015, p. 130. Vgl. over de algemene bekendheid van het risico van skimming: Rb. 's-Hertogenbosch 24 februari 2011 (ktr.), ECLI:NL:RBSHE:2011:BP5939, r.o. 8. Zie uitvoerig over algemeen bekende risico's: Jansen 2012, p. 420-425.

74. Rb. Rotterdam 5 november 2015, ECLI:NL:RBROT:2015:9378 (*X/Rabobank*), r.o. 5.4. Zie ook N.S. van der Meulen, 'Eigen schuld, dikke bult? Aansprakelijkheid bij fraude met internetbankieren', *Informatiebeveiliging* 2012, afl. 8, p. 10.

75. Keirse 2003, p. 43, p. 187; Asser/Sieburgh 6-II 2017/125.

76. Rb. Utrecht 12 augustus 2009, ECLI:NL:RBUTR:2009:BJ5273 (*X/Agis*), r.o. 4.6.

77. Baas & Van Rest 2012, p. 267.

beschermen door alleen verbinding te maken met vertrouwde netwerken of door het adres van websites te controleren.⁷⁸ Ook valt te denken aan het gebruik van beschermende software op een computer, zoals een firewall en antivirusprogramma's. Hij dient deze software en zijn browsers bovendien te updaten.⁷⁹ Dergelijke maatregelen kunnen bijvoorbeeld voorkomen dat een crimineel ransomware kan installeren als de betrokkene klikt op een link of een geïnfecteerd bestand opent in een moeilijk te herkennen phishing-mail, bijvoorbeeld omdat de e-mail persoonlijk aan de betrokkene is gericht door het gebruik van naam en klantnummer, die is opgesteld met behulp van bij de verwerkingsverantwoordelijke buitgemaakte persoonsgegevens. Het geheel ontbreken van basale beveiligingsmaatregelen bij de betrokkene leidt niet automatisch tot de conclusie dat er sprake is van een aan de betrokkene toerekenbare omstandigheid, maar kan wel een belangrijke factor zijn bij de beoordeling of hier sprake van is.

Het zal overigens niet snel voorkomen dat er geen beschermende software door een betrokkene wordt gebruikt of dat software niet *up-to-date* is. Beschermende software is tegenwoordig standaard geïnstalleerd op de meeste apparaten. Ook update een antivirusprogramma of browser zich meestal vanzelf, tenzij de betrokkene automatische updates handmatig uitzet. Buiten het geval dat een betrokkene deze basale beveiligingsmaatregelen niet neemt, of deze zelfs actief verhindert, zal er daarom niet snel sprake zijn van eigen schuld door het ontbreken van anticiperende beveiligingsmaatregelen.

5. Synthese en conclusie

In deze bijdrage beantwoord ik de volgende onderzoeksvraag:

Wanneer kwalificeert een gedraging van de betrokkene als een "omstandigheid die aan de benadeelde kan worden toegerekend" in de zin van art. 6:101 lid 1 BW?

Ik heb de 'toerekenbare omstandigheid' gelijkgesteld aan onzorgvuldig gedrag van de betrokkene ten aanzien van zijn persoonsgegevens. Vervolgens heb ik het (mogelijk onzorgvuldige) gedrag van de betrokkene in drie categorieën onderverdeeld. Deze categorieën zijn: (i) de verwerkingsverantwoordelijke adviseert maatregelen maar de betrokkene volgt deze niet op; (ii) een onzorgvuldig handelen van de betrokkene (zonder dat er sprake is van een advies van de verwerkingsverantwoordelijke); (iii) de betrokkene nam geen anticiperende maatregelen. Ik heb per categorie beoordeeld wanneer het

gedrag van de betrokkene (mogelijk) onzorgvuldig is, en daarmee een toerekenbare omstandigheid in de zin van art. 6:101 lid 1 BW oplevert bij een onrechtmatige verwerking van persoonsgegevens.

Ik kom tot de conclusie dat er vóór, bij of na een onrechtmatige verwerking van persoonsgegevens niet snel sprake is van onzorgvuldig gedrag van de betrokkene of een aan hem toerekenbare omstandigheid. Het inroepen van een eigen schuld-verweer door de aansprakelijke verwerkingsverantwoordelijke zal daarom niet snel leiden tot een andere verdeling van de schade. De verwerkingsverantwoordelijke heeft een stevige zorgplicht te vervullen voordat hij de betrokkene onzorgvuldig gedrag kan verwijten. Het uitgangspunt is namelijk dat de verwerkingsverantwoordelijke de betrokkene proactief en op adequate wijze moet informeren en waarschuwen voordat het gedrag van de betrokkene kwalificeert als onzorgvuldig (paragraaf 4.2.). Op dit uitgangspunt is echter een uitzondering mogelijk in het (bijzondere) geval waarin de betrokkene ook zonder waarschuwing of advies moet begrijpen dat zijn gedrag tot schade kan leiden (paragraaf 4.3.). In dat geval kwalificeert het gedrag van de betrokkene als een toerekenbare omstandigheid. Hier kan ook sprake van zijn als de betrokkene nalaat om basale beveiligingsmaatregelen te nemen of deze zelfs actief verhindert (paragraaf 4.4.).

De effectiviteit van de AVG wordt niet bedreigd door (overmatige) toepassing van eigen schuld (zie paragraaf 3.3.). Eigen schuld bij een onrechtmatige verwerking van persoonsgegevens zal slechts in een beperkt aantal gevallen door de rechter worden gehonoreerd. Het leerstuk van eigen schuld maakt het verkrijgen van een schadevergoeding bij een onrechtmatige verwerking van persoonsgegevens daarom niet (in veel gevallen) onmogelijk.

78. Zie bijvoorbeeld de 10 vuistregels voor veilig internetten van het Nationaal Cyber Security Centrum: <https://www.ncsc.nl/actueel/factsheets/factsheet-10-vuistregels-voor-veilig-internetten.html>.

79. Het updaten van software is belangrijk, omdat het anders niet alle dreigingen herkent.